FortiCloud v1.15.1
Getting Started Guide

FortiCloud v1.15.1 Getting Started Guide

May 10, 2013

32-1144-185516-20130510

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

The FortiCloud service 2
- Simplified central management for your FortiGate network 2
- Hosted log retention with large default storage allocated 2
- Monitoring and alerting in real time 2
- Customized or pre-configured reporting and analysis tools 2
- Maintain important configuration information uniformly 2
- Service security 3
- FortiCloud Service History 3

Registration and Activation 4
- 1. Registering with Support 4
- 2. Registering and Activating your FortiCloud account 6
- 3. Enabling logging to FortiCloud 8
- 4. Logging into the FortiCloud portal 8
- 5. Upgrading to a 200Gb subscription 9

The FortiCloud Portal 10
- Dashboards 10
- Logs & Archives 11
- Drilldown 12
- Reports 13
- Management 14

Using FortiCloud 15
- Adding a new dashboard with custom charts 15
- Filtering logs to find specific information 15
- Downloading logs 16
- Using drilldown charts to find specific information 16
- Viewing and printing existing reports 16
- Generating scheduled and immediate reports 17
- Creating and configuring a new report with your logo 17
- Checking the status of your registration contract 18
- Adding a new user account to a FortiCloud account 18

FortiCloud Help Guide

This getting started guide is for FortiCloud users who want to instruction on how to set up their FortiCloud service to provide device management and monitoring and remote logging for their FortiGate network.

The FortiCloud service

FortiCloud is a hosted security management and log retention service for the FortiGate® and FortiWifi® product line. It gives you a centralized reporting, traffic analysis, configuration and log retention tool without the need for additional hardware and software.

Simplified central management for your FortiGate network

FortiCloud provides a central web-based management console to manage individual or aggregated FortiGate and FortiWifi devices. Adding a device to the FortiCloud management subscription is straightforward and provides detailed traffic and application visibility across the whole network.

Hosted log retention with large default storage allocated

Log retention is an integral part of any security and compliance program, but administering a separate storage system is burdensome. FortiCloud takes care of this automatically and stores the valuable log information in the cloud. Each device is allowed up to 200Gb of log retention storage. Different types of logs can be stored including Traffic, System Events, Web, Applications and Security Events.

Monitoring and alerting in real time

Network availability is critical to a good end-user experience. FortiCloud enables you to monitor your FortiGate network in real time with different alerting mechanisms to pinpoint potential issues. Alerting mechanisms can be delivered via email.

Customized or pre-configured reporting and analysis tools

Reporting and analysis are your eyes and ears into your network's health and security. Pre-configured reports are available, as well as custom reports that can be tailored to your specific reporting and compliance requirements. For example, you may want to look closely at application usage or web site violations. The reports can be emailed as PDFs and can cover different time periods.

Maintain important configuration information uniformly

The correct configuration of the devices within your network is essential to maintaining an optimum performance and security posture. In addition, maintaining the correct firmware (operating system) level allows you to take advantage of the latest features.

Service security

All communication (including log information) between the devices and the clouds is encrypted. Redundant data centers are always used to give the service high availability. Operational security measures have been put in place to make sure your data is secure — only you can view or retrieve it.

FortiCloud Service History

The activation of the FortiCloud service is dependent on the FortiGate model number and firmware release. Before release 5.0 the service was called FortiGuard Analysis and Management Service (FAMS). Unless otherwise stated the use of the term FAMS and FortiCloud is generally interchangeable.

FortiGate Release 3.6 and below

FortiCloud is not supported on releases 3.6 and below.

FortiGate Release 3.6 to 4.3.6

FortiCloud activation is via the FortiGate GUI. Several settings are required to activate and enable the service.

- Models 600 to 800 must activate through the CLI Console.
- The license is Account-based

FortiGate Release 4.3.7 to 4.3.12

FortiCloud activation is via the FortiGate GUI, or via a widget in the FortiGate systems dashboard. Several settings are required to activate and enable the service.

- Models 600 to 800 must activate through the CLI Console.
- The license is Account-based

FortiGate Release 5.0 and above

FortiCloud activation is via a widget in the FortiGate systems dashboard.

- Model 600 to 800 used the CLI to activate.
- The license is device based

Registration and Activation

There are five key activation steps. The procedure for each step may vary depending on your model and your FortiOS firmware version, and whether your device (FortiGate or FortiWifi) is brand new.

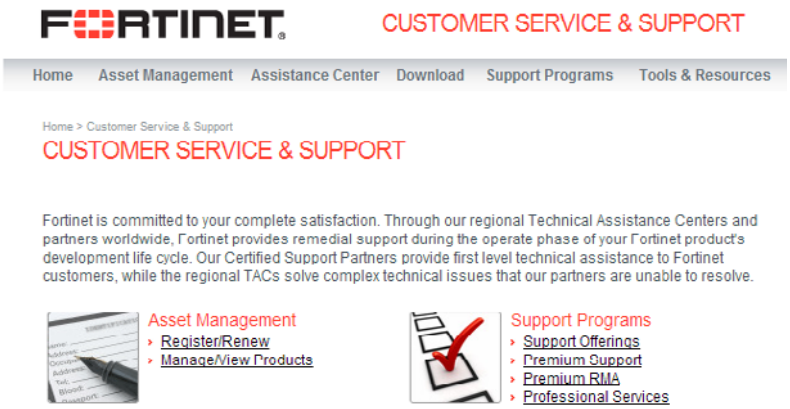
The steps are:

1. Registering with Support (New devices only)
2. Activating your FortiCloud account
3. Enabling logging to FortiCloud
4. Logging into the FortiCloud portal
5. Upgrading to a 200Gb subscription (Recommended)

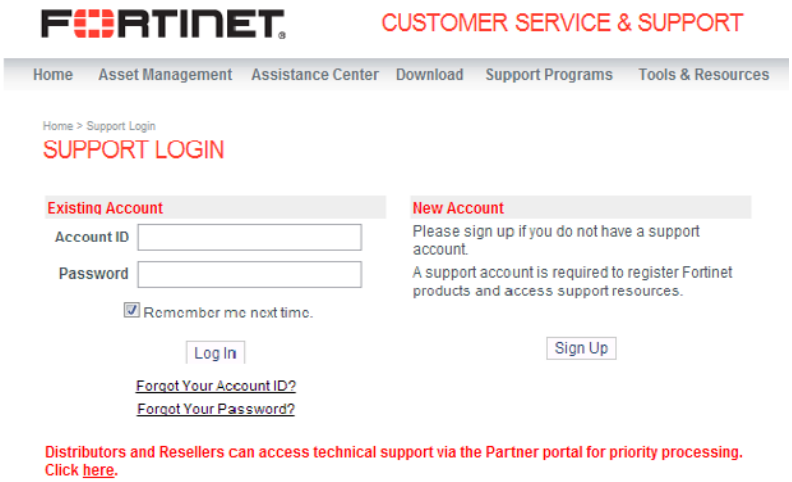
1. Registering with Support

For new devices, registration is very important, as it allows interaction with the Fortinet back-end systems such as support. This registration will also allow other services such as support and data space expansion contracts to be used with your FortiCloud account.

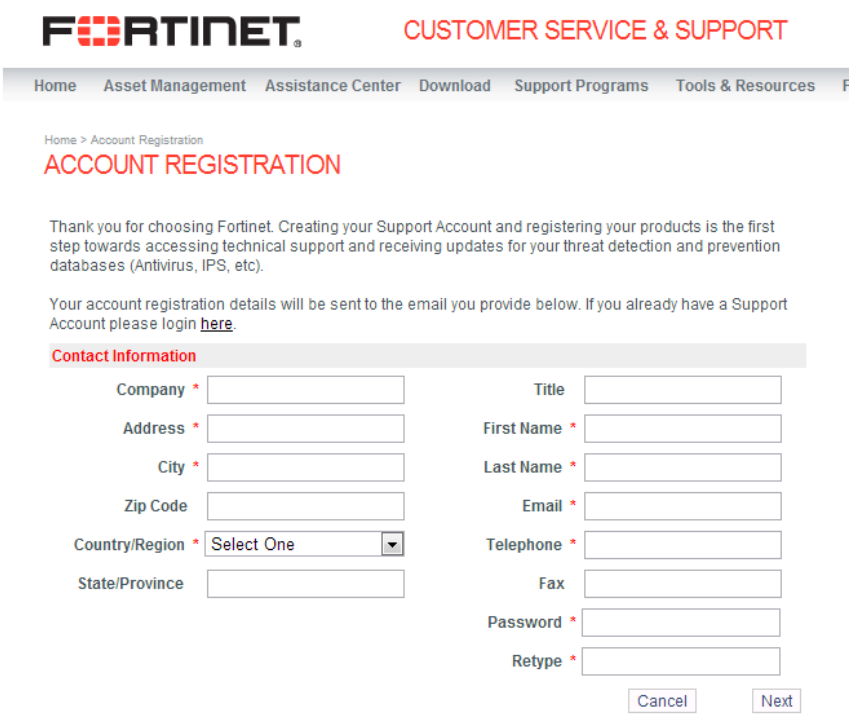
1. Visit https://support.fortinet.com.



2. Select *Register/Renew*.



3. If you do not already have an account, select *Sign Up* under 'New Account'. If you do, enter your information and log in.



4. Select *Register/Renew* again, and follow the process to register your device.

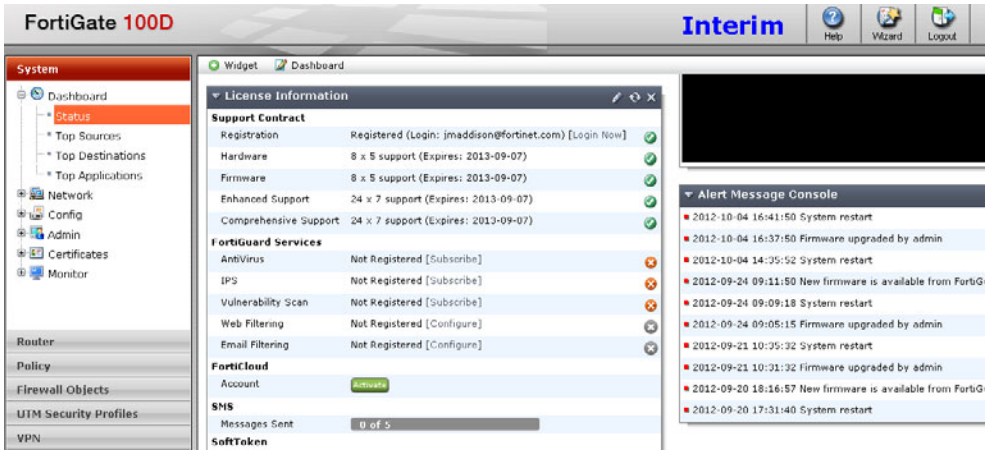
Upgrading to the latest firmware is recommended with both new and existing devices, as it ensures the newest features and fixes will be available, and that the FortiCloud Service will be receiving all of the logging information from your FortiGate unit. You can upgrade from the Support homepage, or using the FortiExplorer program.

2. Registering and Activating your FortiCloud account

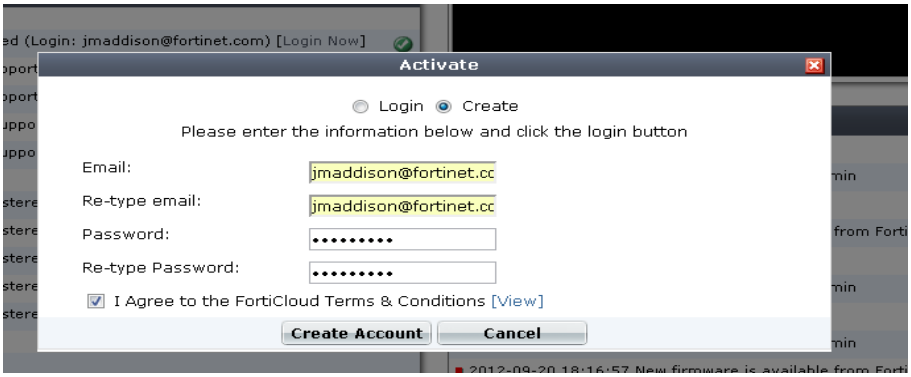
FortiCloud accounts can be registered manually through the FortiCloud website, https://www.forticloud.com. But you can easily register and activate your account directly within your FortiGate unit. Your registration process will vary somewhat depending on which firmware version and device you have.

FortiOS 5.0 (FortiGate 300 and below, all FortiWifi units)

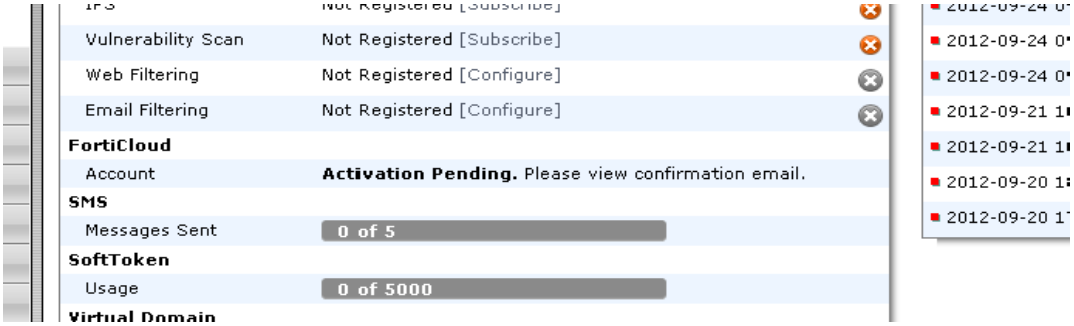
1. On your device's dashboard, in the License Information widget, is a green 'Activate' button. Press it.



2. A dialogue asking you to register your FortiCloud account will appear. Enter your information, view and accept the Terms and Conditions, and select *Create Account*.



3. A second dialogue window will appear, asking you to enter your information to confirm your account. This will send a confirmation email to your registered email. The dashboard widget will update to show that confirmation is required.



4. Open your email, and follow the confirmation link contained in it.

A FortiCloud page will open, stating that your account has been confirmed. The Activation Pending message on the dashboard will change to state the type of account you have ('1Gb Free' or '200Gb Subscription'), and will now provide a link to the FortiCloud portal.

FortiOS 3.6 to 4.3.12 (FortiGate 300 and below, all FortiWifi units)

The registration process and dashboard information is largely the same as 5.0, although the interface may still refer to the service by its former name, FAMS (FortiGuard Analysis and Management Service).

FortiGate 600 to 800

For 600 through 800, FortiCloud registration must be done through the FortiGate CLI Console.

Devices beyond the FortiGate 800 do not support the FortiCloud service.

3. Enabling logging to FortiCloud

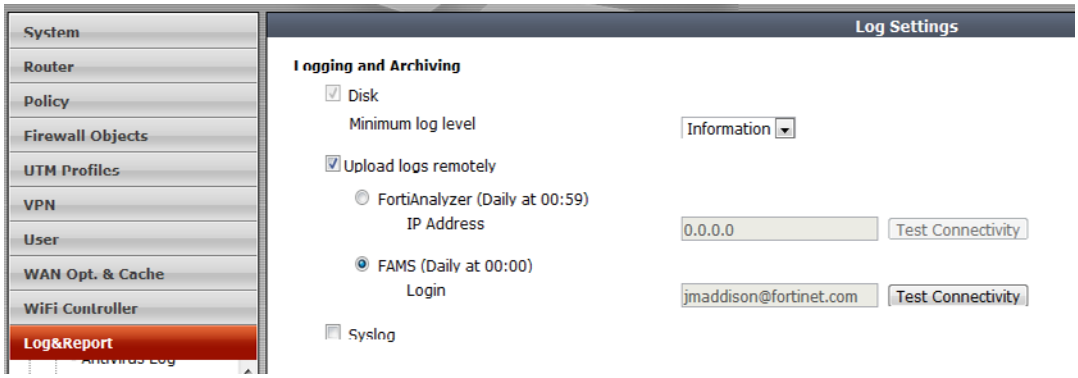
In order to enable remote logging to the FortiCloud Service, you must first configure the FortiGate's log uploading settings. You must also enable logging in each policy that covers traffic that you want to be logged.

FortiOS 5.0

FortiOS 5.0 will automatically start logging Traffic and Event logs to FortiCloud upon activation. Logging can be disabled or configured through the FortiGate interface or CLI Console.

FortiOS 4.3 (and earlier)

1. Open the Log & Report section in the FortiGate interface, and select Log Setting.



2. Enable 'Upload logs remotely'.
3. Select FAMS, and enter your username in the text box.
4. Select *Test Connectivity* to ensure the service is working.

Configuring policies (5.0 and 4.3)

After enabling logging functionality, you will need to select which policies will be logged.

1. Open the Policy list.
2. Choose the policy you would like to log, and select *Edit*.
3. Check the box next to *Log Allowed Traffic*.
4. Select *Submit*.

4. Logging into the FortiCloud portal

Once logging has been configured and you have registered your account, you can log into the FortiCloud portal and begin viewing your logging results. There are two methods to reach the FortiCloud portal:

- If you have direct networked access to the FortiGate unit, you can simply open your Dashboard and check the License Information widget. Next to the current FortiCloud connection status will be a link to reach the FortiCloud Portal.
- If you do not currently have access to the FortiGate's interface, you can visit the FortiCloud website (https://www.forticloud.com) and log in remotely, using your email and password. It will ask you to confirm the FortiCloud account you are connecting to, and then you will be granted access. Connected devices can be remotely configured using the Scripts page in the Management Tab, useful if an administrator may be away from the unit for a long period of time.

5. Upgrading to a 200Gb subscription

Upgrading is simple, but must be done through the FortiGate unit, as the storage contract is allocated based on devices, rather than user accounts.

1. Open the FortiGate Dashboard.
2. In the License Information widget, select *Upgrade* next to 'Type' in the FortiCloud section.
3. A new window will open, showing the Fortinet Support portal. Follow the onscreen instructions to register your contract.
4. Wait approximately 10 minutes for the contract to be applied, and then visit your Dashboard.

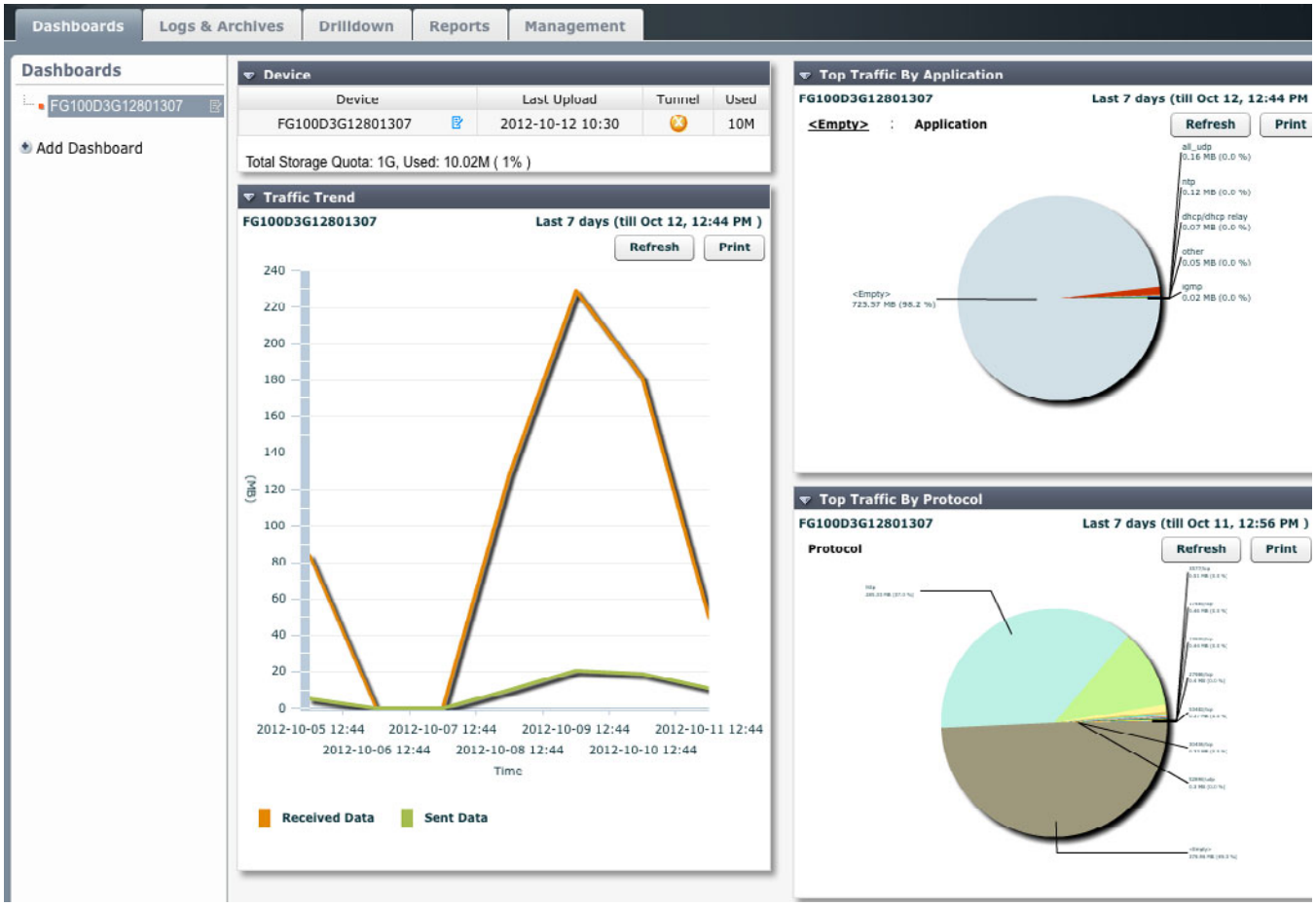
In the License Information widget, Type will have changed from 'Free' to 'Subscribed'. Your maximum listed storage will also have updated.

The FortiCloud Portal

There are five main tabs in the FortiCloud portal, which allow you to access different features and information. The FortiCloud Settings, Help, and Logout buttons appear in the upper right.

- Dashboards
- Logs & Archives
- Drilldown
- Reports
- Management

Dashboards

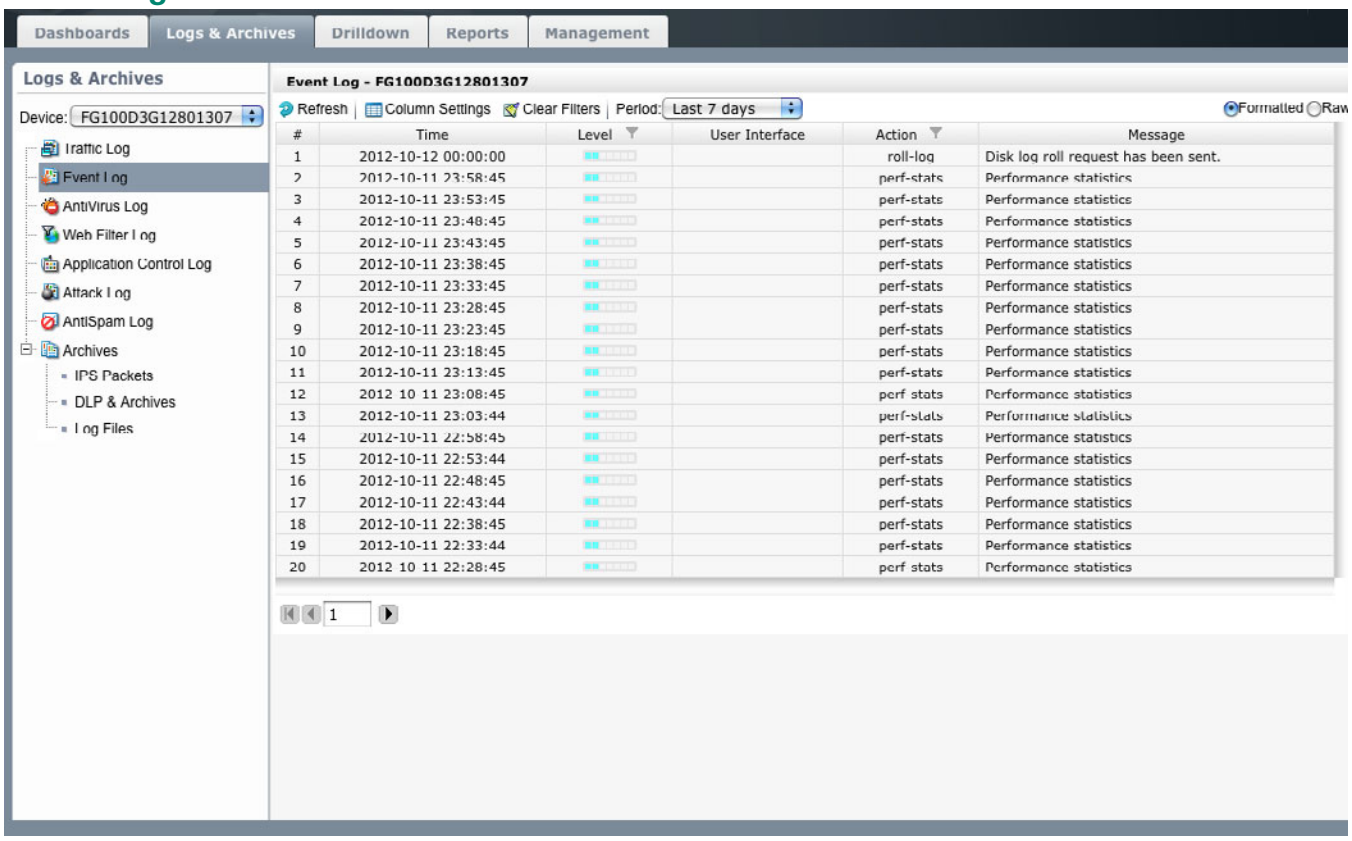


The Dashboards Tab provides you with a general overview of the information from recent logs, with charts and widgets to provide background info and show you trends. The charts can be interacted with for more info.

Left-hand column: a list of the current dashboards available. The default setup is a dashboard for each device.

Main window: the dashboard content, made up of configurable widgets and charts.

Logs & Archives



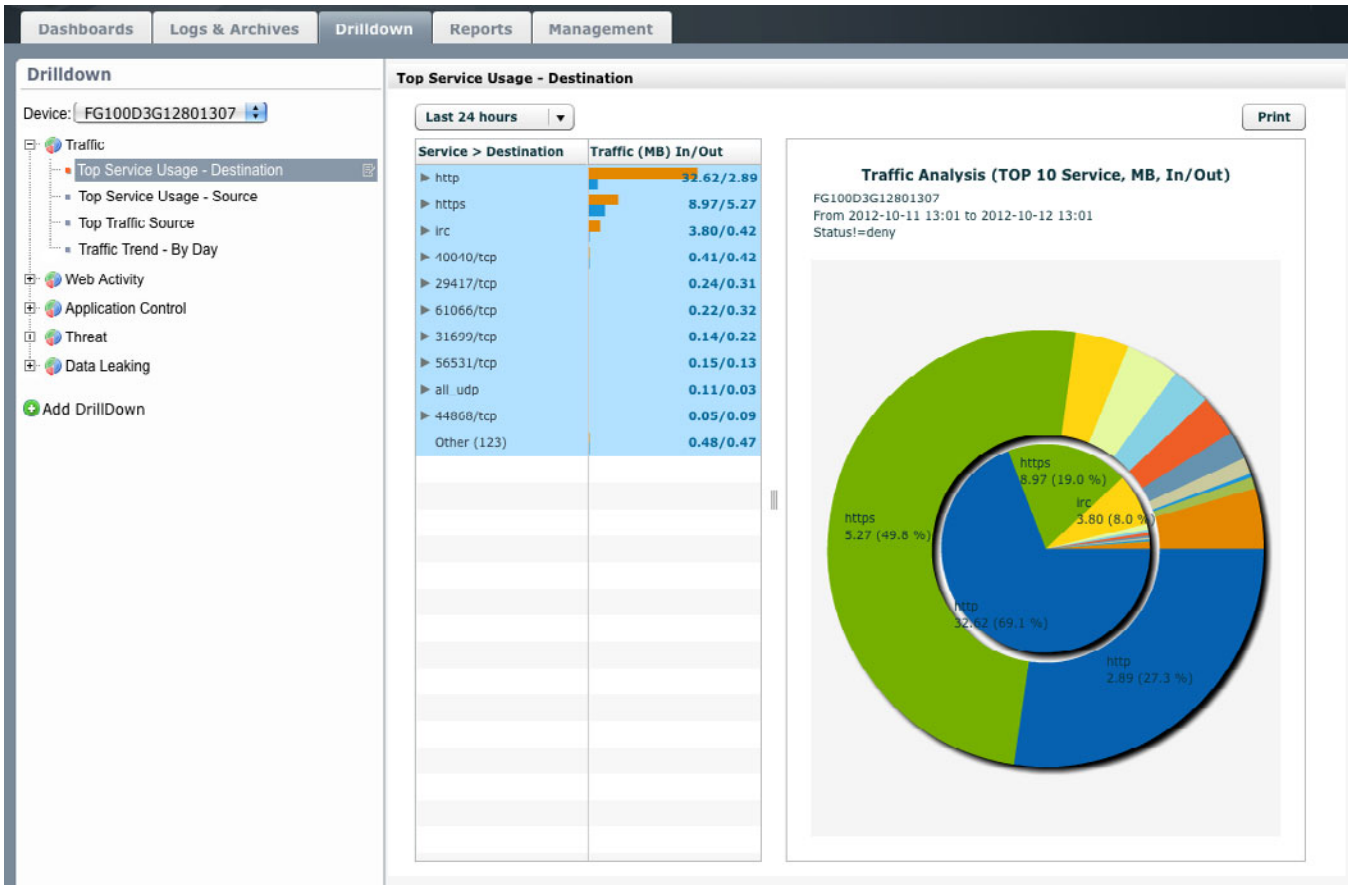
The Logs & Archives Tab lists all of the individual logged messages, divided by category. The log information can be customized and filtered, and Raw (unformatted) logs can be viewed.

Left-hand column: a list of the log types and archives available to view.

- Traffic Log: Lists all logged traffic passing through the device.
- Event Log: Lists admin and user activity and other internal device info.
- Antivirus Log: Lists virus incursions and AV activity records.
- Web Filter Log: Lists web filter actions, notifications and monitoring records.
- Application Control Log: Lists controlled, monitored, and blocked application records.
- Attack Log: Lists network attack records.
- Anti-Spam Log: Lists email protection service records.
- Archives: Lists IPS and DLP records, and allows you to download raw log files.

Main window: the currently selected log type's content, with log data divided by customizable columns.

Drilldown



The Drilldown Tab is where you can find more information on any particular topic. The information is automatically extracted and charted from the logs the FortiGate unit has uploaded, and the charts can be interacted with to see finer details.

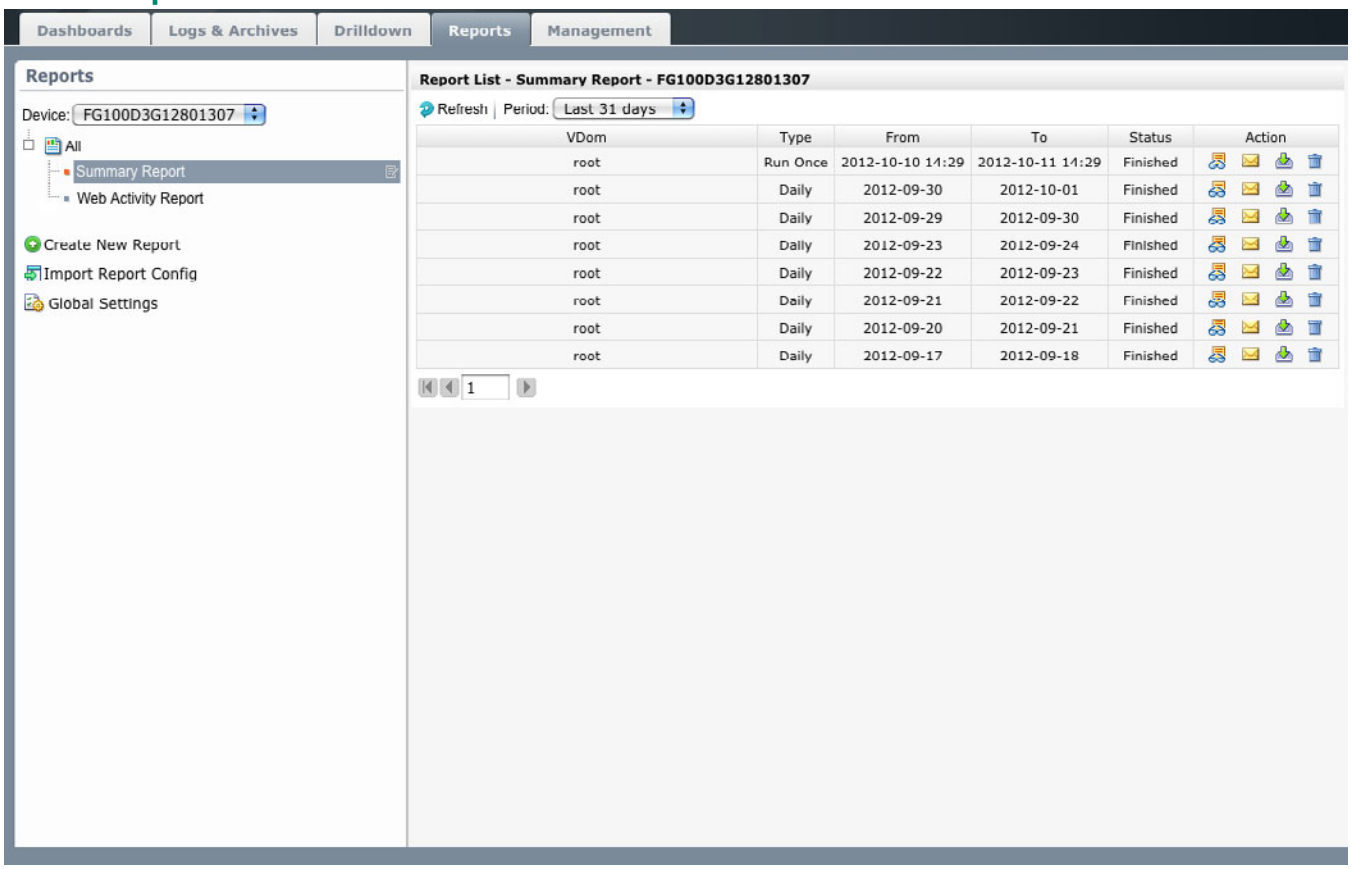
Left-hand column: a list of the drilldown chart types, each with several chart subtypes available.

- Traffic: details about traffic types, sources, and usage.
- Web Activity: details about popular web categories and sites.
- Application Control: details about blocked and monitored applications.
- Threat: details about viruses, spam, and network attacks.
- Data Leaking: details about DLP activity.

UTM drilldowns such as Application Control will only list information if a connected FortiGate or other device has the UTM function enabled on a policy that is currently being logged.

Main window: the currently selected Drilldown's information, with the data listed on the left and charted on the right.

Reports



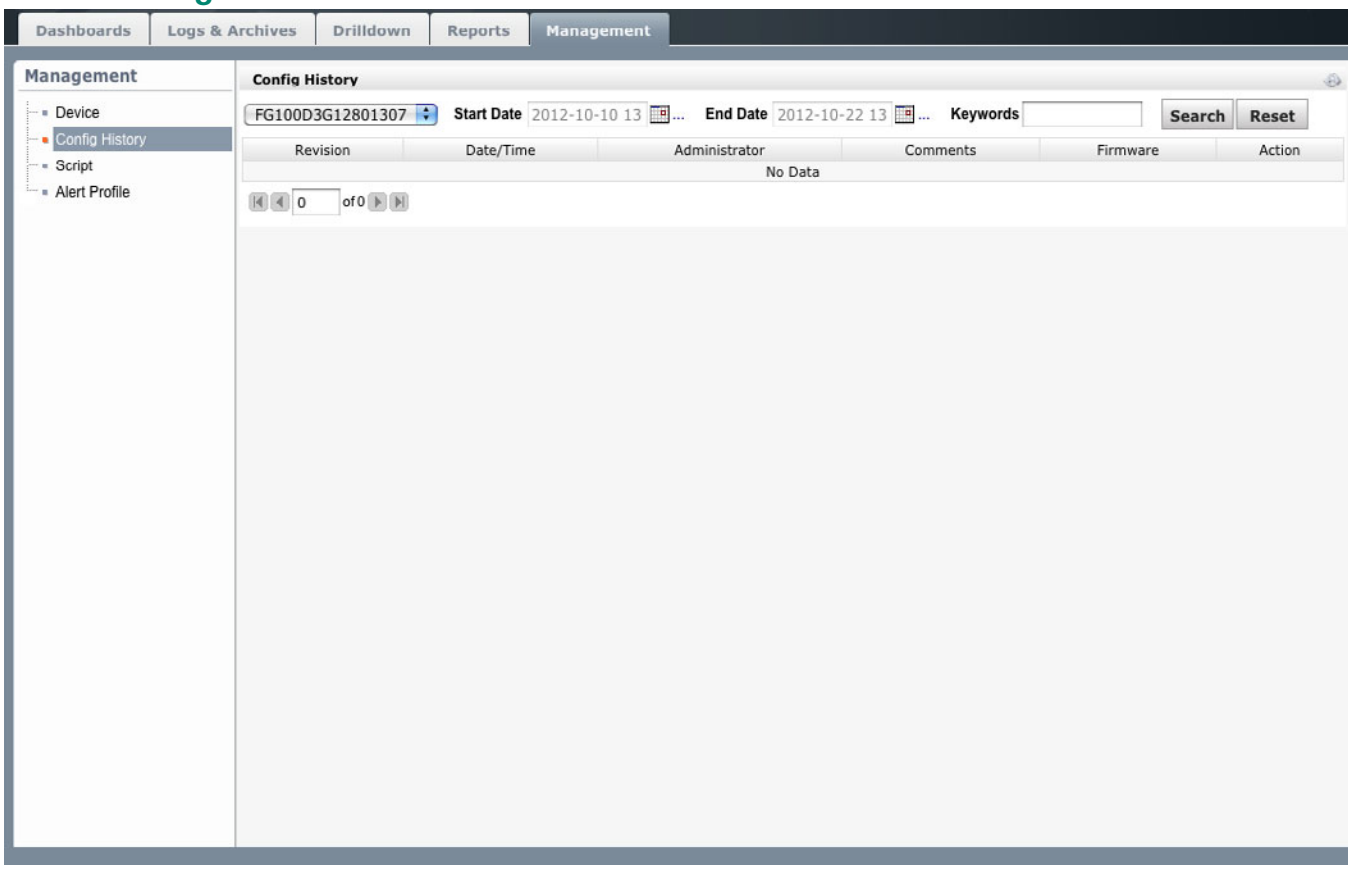
The Reports Tab is where you can find all published logging reports, as well as configure report styles and scheduling for future reporting. You can also import and export existing report styles, useful for standardization.

Left-hand column: a list of available report styles, as well as report configuration options.

- Summary Report: a general overview of UTM and traffic information.
- Web Activity Report: a report with a focus on traffic sources and destinations.

Main window: a list of available reports in the currently selected style, with detailed report information and buttons for viewing and moving reports at the far right.

Management



The Management Tab consists of four sections, each for controlling different features of FortiCloud. This tab will be most useful to clients with large numbers of devices, as it tracks device information, allows you to run scripts to the devices remotely, and configures conditions for sending alert emails, useful for notifying remote administrators of various problems.

Left-hand column: options for managing and viewing different information and functions of the FortiCloud Portal:

- Device: lists all connected devices, and offers additional info and options for each one.
- Config History: lists FortiCloud configuration changes, and allows you to roll back.
- Script: sends console scripts to the linked devices remotely.
- Alert Profile: controls alert email send conditions and messages.

Main window: the information/settings for the selected option.

Using FortiCloud

Below is a list of possible tasks that show you how to make the best of the features that FortiCloud has to offer.

Tasks:

- Adding a new dashboard with custom charts
- Filtering logs to find specific information
- Downloading logs
- Using drilldown charts to find specific information
- Viewing and printing existing reports
- Generating scheduled and immediate reports
- Creating and configuring a new report with your logo
- Checking the status of your registration contract
- Adding a new user account to a FortiCloud account

Adding a new dashboard with custom charts

Creating multiple dashboards to show different kinds of data is simple. You could have a dashboard to cover a particular kind of threat, or have a dashboard for each loggable device (if you have multiple devices connected to your FortiCloud account).

1. Open the Dashboard Tab.
2. In the Dashboards column on the left, select *Add New Dashboard*.
3. Next to the name 'New Dashboard' is the Edit icon. Select it.
4. Select one of the options from the list:
   - Select *Add Widgets* to add a widget or chart. You will select one from a list, and another window will appear allowing you to customize it before it appears on the dashboard.
   - Select *Change Layout* to change the design of your dashboard.
   - Select *Rename* to rename the Dashboard.

Filtering logs to find specific information

In the Logs & Archives Tab, you can filter log information in order to find specific records, and select individual log messages to see even more information about their content.

For this example, you'll be looking for FortiGate reboot logs, to monitor when the FortiGate unit has been reset.

1. Open the Logs & Archives Tab.
2. Select the log you'd like to search in from the column on the left, such as the Event Log.
3. At the top of the Action column, next to the column title, is a funnel icon. Select it.

If the Action column is not visible, select 'Column Settings' above the log list and add it to the list of displayed columns.

4. You will see a list of all the keywords that can appear in the Action column. Find 'reboot' in the list, and select the right arrow button to move it into the 'Display Fields' column.
5. Select *Submit*. The page will refresh to only display 'reboot' logs, such as those that occur after a factory reset.
6. Mouse over one of the logs to highlight it, and click to open a window listing all of the log details.

Downloading logs

In the Logs & Archives Tab, you can download all recorded log data for any of the log categories. Regular archiving and backing up of data can help maintain a complete network history.

1. Open the Logs & Archives Tab.
2. Select the Archives section in the left-hand column.
3. Select Log Files below Archives.
4. You will see a list of all the logs the service has recorded, divided by category.
5. Choose the log you would like to download, and select the Download icon from the *Action* column on the far right.

Using drilldown charts to find specific information

The Drilldown Tab provides many useful charts, and the ability to add more, but the charts themselves contain more in-depth information. You can select any chart element that is highlighted when the mouse passes over it in order to get more info. Custom Drilldowns can be added, much like charts to the Dashboard.

For this example, you'll be looking for at top traffic sources in the last 24 hours. If your network is being hammered with constant traffic, you could use the chart to see what the source address of the traffic is.

1. Open the Drilldown Tab.
2. Select *Traffic* from the list of Drilldown categories in the left column. A few preset Traffic Drilldowns will appear.
3. Select 'Top Traffic Source' from the list.
4. The chart is likely empty, because the default time period is 'Last 60 minutes'. Open the dropdown list above the charts and select 'Last 24 hours'.
5. The chart will refresh and show the new information. At the top is the IP with the most traffic. Select it to open the list of IPs it has shared traffic with.
6. The chart on the right will refresh again, and show just the information for that selected IP, with colums displaying in and out traffic paired together, with listed amounts in Mb.

Viewing and printing existing reports

Reports give you specific breakdowns of log information gathered over periods. They can be configured and created, but some default styles are provided for you to use. They can be viewed, configured, downloaded, and printed from within the FortiCloud portal.

1. Open the Reports Tab.
2. Select one of the Report types from the list in the left column to see the list of those reports in the main window. If none appear, you may have to change the *Period* dropdown to a longer period of time.
3. You will see a list of all generated reports within the period. The four icons at the far right allow you to View, Email, Download, and Delete reports. Select the View icon.
4. The report will open in a popup window for you to view.
5. You can then either print directly from your browser, or go back and Download the report and print the PDF file from your computer.

Generating scheduled and immediate reports

Reports are generated daily by default and emailed to the address used to register for FortiCloud. You can change the schedule to be Daily, Weekly, or Monthly (or any combination of those), and set whether reports should be emailed upon generation or not. They can also be generated on command if you need the information immediately.

1. Open the Reports Tab.
2. Select the report type you want to generate or configure from the list in the left column.
3. A small Edit icon will appear after the selected report type's name in the column, once it is selected. Click on it to open the list of options, and select the option you need.
   - *Edit* will let you edit the report's contents and structure.
   - *Copy* creates a duplicate of the report style that can be edited without changing the original.
   - *Schedule* sets the scheduling settings for the report: how often the reports are automatically made, whether they are emailed or not, and which VDOM the reports will gather the log information from.
   - *Run Report* tells FortiCloud to immediately generate a report. It will appear in the column with a Status of 'Scheduled', and will take a few minutes to generate before it is available to view.
   - *Delete* deletes the report style from the list.
   - *Export* creates a report configuration file that contains only the report's style information. It can be imported to any FortiCloud to get identically structured reports using the *Import Report Config* button, further down the left-hand column.
4. Select *Schedule* to change the scheduled generation of reports, or select *Run Report* to immediately generate a report.

Creating and configuring a new report with your logo

If you are looking to track and report on specific information not covered in the standard reports, you can create a new report with the content you choose. You can also choose a logo image that will be applied to all reports generated in future by the FortiCloud Service, to brand your results.

1. Open the Reports Tab.
2. Select *Create New Report* from the left-hand column.
3. Enter the desired filename and title for the report.
4. Select any of the three 'Add' commands to add new information to the report.
   - *Add Chart* adds a new chart, opening a window to configure what information the chart should be visualizing. You can create a chart's options from scratch, or select *Choose a Predefined Chart* next to the Chart Name box to start with a preset chart style that can then be customized.
   - *Add Section Title* adds a title header to the report, which can be used to divide up the report into sections.
   - *Add Description* allows you to add a text box with any text you choose, which can be used to further explain the information in a chart, or provide any text content you choose.
5. Click and drag any of the added objects' title bars to reorder them.
6. Once you're satisfied with the report style, select *Save* at the bottom.
7. Select the new report style from the list, and use Run Report (explained above) to generate a sample of the new report. Wait for it to finish, and you can view it from the report list.

Checking the status of your registration contract

The FortiCloud service comes with a default 1 Gb (1024 Mb) of server space per linked device for your log information. For multiple devices with real-time logging and automatic reports, that space can fill quickly. You can make a registration contract through the FortiCare support service at https://support.fortinet.com for more space, up to 200Gb per unit.

Once you've made a contract, you can register your contract in the FortiCloud interface so it will track how much space has been used and how long you have until the contract must be renewed.

1. Select the Options menu (the gear icon) from the upper right of the FortiCloud portal.
2. Select *Contracts* from the list.
3. If you have a contract that is not registered in the portal yet, you will have received a code. Enter the code in the box and select *Add Contract*.
4. If you do have a contract registered, the current used/maximum space, length of contract term, and start and end dates of contract term will be listed here for you to view.

Adding a new user account to a FortiCloud account

You may require multiple Administrators to have access to a FortiCloud portal, or may want specific users to be able to view the log data without making changes (known as Viewers in the FortiCloud portal). You can register any email account as a user from within the FortiCloud portal, and select a role for the user to dictate what content they can view and edit.

1. Select the *Options* menu (gear icon) from the upper right of the FortiCloud portal.
2. Select *Users* from the list.

A list of current users and their roles will appear. The email/user that registered the FortiCloud account is permanently an Administrator and cannot be removed.

3. In the upper right of the popup, next to the red Close button, is a link titled *Add User*. Select it.
4. Fill in the desired user's Email, Username, and Password, and choose the role (Admin, Viewer, etc) and language you'd like them to use.
5. Select *Submit*.

The user will receive a confirmation email to their account address. They will be required to visit a link within that email before their account can be used. After that, they may login any time from https://www.forticloud.com.